AMENDMENTS TO THE CLAIMS

Please amend claims 1, 9, 16 and 23 as follows:

1. (Currently Amended) A network security system comprising:

a first distributed software agent comprising a processor configured to collect a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

a second distributed software agent comprising a processor configured to collect a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock; and

a manager module in communication with the distributed software agents, the manager module comprising a processor configured to:

receive the first and second stream of alerts;

identify a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address;

determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

if the first clock and the second clock are not synchronized:

synchronize the first clock and the second clock;

modify at least one of a timestamp within the first alert and a timestamp within the second alert; and

~~correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule.~~

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

2. (Previously Presented) The network security system of claim 1, wherein the manager module synchronizes the first clock and the second clock by determining a synchronization error using the time of detection included in the first alert and the time of detection included in the second alert, and correcting the synchronization error.

3. (Original) The network security system of claim 1, wherein the manager module synchronizes the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock.

4. (Original) The network security system of claim 3, wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock.

5. (Previously Presented) The network security system of claim 1, wherein the manager module synchronizes the first clock and the second clock by adjusting a time offset associated with the first clock.

6. (Cancelled)

7. (Previously Presented) The network security system of claim 1, wherein the second alert corroborates the first alert.

8. (Original) The network security system of claim 1, wherein the first network security device comprises an Intrusion Detection System (IDS).

9. (Currently Amended) A method performed by a network security system, the method comprising:

receiving a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

receiving a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock;

identifying a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address;

determining, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

if the first clock and the second clock are not synchronized:

synchronizing the first clock and the second clock;

modifying at least one of a timestamp within the first alert and a timestamp within the second alert; and

~~correlating the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule.~~

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determining whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

10. (Previously Presented) The method of claim 9, wherein synchronizing the first clock and the second clock comprises determining a synchronization error using the time of detection included in the first alert and the time of detection included in the second alert, and correcting the synchronization error.

11. (Original) The method of claim 9, wherein synchronizing the first clock and the second clock comprises selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock.

12. (Original) The method of claim 11, wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock.

13. (Original) The method of claim 9, wherein synchronizing the first clock and the second clock comprises adjusting a time offset associated with the first clock.

14. (Cancelled)

15. (Previously Presented) The method of claim 9, wherein the second alert corroborates the first alert.

16. (Currently Amended) A machine readable medium storing a set of instructions that, when executed by the machine, cause the machine to:

receive a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

receive a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock;

identify a first alert in the first stream and a second alert in the second stream wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address;

determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

if the first clock and the second clock are not synchronized:

synchronize the first clock and the second clock;

modify at least one of a timestamp within the first alert and a timestamp within the second alert; and

~~correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the second alert satisfy a condition of the rule.~~

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

17. (Previously Presented) The machine readable medium of claim 16, wherein synchronizing the first clock and the second clock comprises determining a synchronization error using the time

of detection included in the first alert and the time of detection included in the second alert, and correcting the synchronization error.

18. (Original) The machine readable medium of claim 16, wherein synchronizing the first clock and the second clock comprises selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock.

19. (Original) The machine readable medium of claim 18, wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock.

20. (Original) The machine readable medium of claim 16, wherein synchronizing the first clock and the second clock comprises adjusting a time offset associated with the first clock.

21. (Cancelled)

22. (Previously Presented) The machine readable medium of claim 16, wherein the second alert corroborates the first alert.

23. (Currently Amended) A network security system comprising:

a plurality of distributed software agents, each comprising a processor configured to

collect alerts from a plurality of corresponding network security devices, each network security device having a clock; and

a manager module in communication with the distributed software agents, the manager module comprising a processor configured to:

receive the alerts;

identify alerts from a subset of the plurality of network security devices, wherein all of the identified alerts include a particular Internet Protocol (IP) address;

determine, based on the identified alerts, whether the clocks of the subset of the plurality of network security devices are synchronized; and

if the clocks of the subset of the plurality of network security devices are not synchronized:

synchronize the clocks of the subset of the plurality of network security devices;

modify at least one of a timestamp within a first identified alert and a timestamp within a second identified alert; and

~~correlate the first identified alert and the second identified alert according to a rule, which comprises determining whether the first identified alert and the second identified alert satisfy a condition of the rule.~~

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

24. (Previously Presented) The network security system of claim 23, wherein the manager module synchronizes the clocks of the subset of the plurality of network security devices by adjusting timestamps in each alert received from the subset of the plurality of network security devices.

25. (Previously Presented) The method of claim 9, further comprising causing the event represented by the first alert to occur.

26. (Previously Presented) The method of claim 25, further comprising causing the event represented by the second alert to occur.